Bundesakademie
für Sicherheitspolitik

BAKS - Arbeitspapiere 3/23

Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung

von Regine Grienberger

Bei einem Cyberangriff ist die Identität der Angreifer oft nicht unmittelbar klar und die Tat damit für Staaten oder nichtstaatliche Akteure zunächst abstreitbar. Hier setzt Attribution an: Ist eine technische Ermittlung erfolgt, woher eine Attacke im Cyberraum kommt, stellt sie einen möglichst eindeutigen Zusammenhang her und schreibt die Tat einem Verursacher zu. In Deutschland hat die Bundesregierung dazu 2021 ein nationales Attributionsverfahren eingeführt. Welche Chancen und Risiken birgt Attribution im Cyberraum, und wie sind die ersten Erfahrungen mit dem deutschen Verfahren?

Konflikte zwischen Staaten werden heute auch im Cyberspace ausgetragen; mit Spionage-, Sabotage- und Subversions-Operationen versuchen Staaten, Vorteile zu erlangen oder einem anderen Staat zu schaden. Anders als bei einem konventionellen Angriff kann bei einer Cyberattacke allerdings die eigentliche Durchführung verborgen bleiben, und selbst, wenn der Angriff selbst aufgedeckt wird, ist die Identität des Angreifers nicht unmittelbar klar. Genau dies ist häufig der Grund, warum die Wahl auf Cybermittel fällt: Die Verantwortung für die Tat selbst kann abgestritten werden („*deniability*"), und wenn der Verursacher in Deckung bleibt, muss er auch keine Reaktion befürchten.

Hier setzt Attribution an: Sie etabliert einen möglichst eindeutigen Zusammenhang, benennt die Tat und schreibt sie einem staatlichen oder nichtstaatlichen Akteur zu. Da dies einen Konflikt entfachen oder verschärfen kann, muss das Instrument in verantwortungsvoller Weise gehandhabt werden. Eine maßgebliche Rolle dafür spielt der 2021 vorgelegte VN-Expertenbericht zur Stärkung verantwortlichen Staatenverhaltens im Cyberspace.[1] Die darin formulierte *Norm b* gibt Staaten auf, alle relevanten Informationen zu berücksichtigen, den Kontext des Vorfalls ebenso wie technische Fragen und Auswirkungen: „*States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.*" Auf dieser Norm hat die Bundesregierung das 2021 eingeführte nationale Attributionsverfahren aufgebaut.

Unterschiedliche Arten der Attribuierung

Wie die Bundesregierung attribuiert, hängt von den vorhandenen Informationen zum Cybervorfall ebenso ab wie vom Ziel der Attribution. So muss zunächst entschieden werden, ob öffentlich attribuiert wird, oder auf dem diplomatischen Weg, in der direkten Ansprache des Akteurs, zum Beispiel über die jeweilige Botschaft. Völkerrechtlich gibt es keine Pflicht, eine Attribution öffentlich zu machen. Eine Attribution

[1] Der VN-Bericht ist hier verfügbar: https://disarmament.unoda.org/group-of-governmental-experts/.

auf dem diplomatischen Weg kann als ‚letzte Warnung' ins Spiel gebracht werden, um die andere Seite dazu zu bewegen, die Aktivitäten umgehend einzustellen. Eine weitere Funktion ist zu signalisieren: „wir haben euch erwischt", und damit auch die eigenen Detektions- und Abwehrfähigkeiten zu demonstrieren. Wenn hingegen die heimische Öffentlichkeit sensibilisiert werden soll, etwa um auf Verwundbarkeiten im Cyberraum und die Risiken der digitalen Vernetzung aufmerksam zu machen, muss auch öffentlich attribuiert werden. Einen Cybervorfall durch Attribution öffentlich zu machen, kann auch helfen, die erforderlichen Mittel zu mobilisieren, um Systeme sicherer zu machen. Öffentliche Attribution schafft zudem die in einer Demokratie notwendige Transparenz.

Die öffentliche Attribuierung, das ‚*naming and shaming*', macht auf internationaler Ebene die Normverletzung sichtbar. Die eigenen Handlungen auf der Anerkennung von Völkerrecht aufzubauen und Entscheidungen internationaler Tragweite soweit als möglich transparent zu machen, entspricht dem Bekenntnis Deutschlands zur regelbasierten Ordnung und zum Multilateralismus. Indem die Verletzung einer global vereinbarten Norm angezeigt wird, wird diese Norm bekräftigt. Jede Regierung, die Cybervorfälle nach den Ansprüchen von *Norm b* attribuiert, bekennt sich damit zur Geltung des Normenkatalogs insgesamt und stärkt diesen Rahmen. Darüber hinaus erfahren andere und potenzielle Opfer von Versuch oder Erfolg eines Angriffs und können sich selbst besser schützen. Andere und potenzielle Täter werden vom Missbrauch des Cyberraums abgeschreckt: Allein, dass dem Instrument die Abstreitbarkeit entzogen wird, macht es potenziell weniger interessant, denn die durch Cyberangriffe angestrebten Vorteile müssen die Nachteile für die bilateralen Beziehungen, aber auch den Ansehensverlust in der internationalen Gemeinschaft übertreffen.

Eine weitere Entscheidung im Attributionsverfahren ist bezüglich der Solidarisierung mit anderen zu treffen: Soll alleine, als einzelne Regierung, oder gemeinsam mit Partnern attribuiert werden? Ob sich Deutschland in Solidarität der Attribution eines anderen digital angegriffenen Staates anschließt oder selbst andere bittet, die Attribution zu begleiten und zu unterstützen: In beiden Fällen manifestiert sich das gemeinsame Interesse an Stabilität im Cyberraum und damit eine wichtige gemeinsame Handlungsgrundlage. Auch können die Kosten von Retaliationen auf die Mitglieder einer solidarischen Gruppe verteilt werden und damit für jeden einzelnen Staat geringer ausfallen. Im Rahmen des Attributionsverfahrens wird also auf strukturierte Weise über einen Katalog von Handlungsmöglichkeiten entschieden und es werden zur beabsichtigten Wirkung passende Elemente ausgewählt. Dabei kann auch die Nichtnutzung des vorhandenen Instrumentariums eine diplomatische Botschaft senden.

Das nationale Attributionsverfahren der Bundesrepublik

Deutschland steht einem gemeinsamen Vorgehen, insbesondere im Kreis der EU-Mitgliedstaaten, aufgeschlossen gegenüber und hat in allen Attributionsverfahren stets den Schulterschluss mit Partnern gesucht. Trotzdem bleibt Attribution auch aus deutscher Sicht ein nationales Vorrecht. Die Beauftragung einer dritten, neutralen Stelle oder Abgabe an eine übergeordnete, integrierte Institution hat die Bundesregierung bisher stets abgelehnt. Einerseits ist die Attribution als Maßnahme an außen- und sicherheitspolitische Interessen geknüpft – zum anderen sind die Konsequenzen einer Attribution und der mögliche Konflikt mit dem beschuldigten Staat national zu tragen.

Verschiedene Cybervorfälle, die Deutschland direkt betrafen, haben das erforderliche politische Momentum generiert, um ein nationales Attributionsverfahren zu vereinbaren. Dies waren einerseits vor allem der *Hack* der Netze des Bundestags 2015 und des Auswärtigen Amtes 2017, andererseits der Wunsch von Verfassungsschutz, Polizei und Cybersicherheitsfachleuten, die zunehmende Aktivität ausländischer Nachrichtendienste in Deutschland öffentlich zu machen. Daraus ergab sich insbesondere beim Auswärtigen Amt die Forderung nach einem Ansatz, der auch die Einbeziehung außen- und sicherheitspolitischer Überlegungen erlaubt sowie die Einbindung der relevanten Behörden in einem strukturierten Verfahren. Den letzten Anstoß gab der oben genannte VN-Expertenbericht, welcher zu einer verantwortungsvollen Handhabung dieses Instruments in nationaler Souveränität aufruft.

Beteiligte des deutschen Attributionsverfahrens sind das Bundesministerium des Inneren, das Auswärtige Amt, das Bundeskanzleramt sowie das Bundesministerium der Verteidigung und das Bundesministerium der Justiz mit ihren jeweiligen Erkenntnisquellen. Auslöser des Verfahrens kann sowohl ein mutmaßlich durch einen ausländischen Akteur ausgelöster Cybervorfall in deutschen Netzen sein als auch die Bitte eines Verbündeten oder Partners um eine Geste der Solidarität. Jedes der beteiligten Ressorts kann das Verfahren auf der Basis eigener Einschätzung anstoßen. Das Auswärtige Amt als Federführer übernimmt die Durchführung und stellt für jeden Schritt das erforderliche Einvernehmen im Kreis der Bundesregierung her. Da die Reaktion auf einen Cybervorfall direkt die internationalen Beziehungen, sowohl zum beschuldigten Staat als auch anderen Staaten, beeinflusst, ist klar: Bei der Erarbeitung des Handlungsvorschlags muss die Diplomatie im *Lead* sein.

In der ersten Phase werden technische Informationen zusammengetragen, unter anderem durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die deutschen Nachrichtendienste. Es ist wichtig zu verstehen, dass auf Grund der technischen Beschaffenheit des Cyberspace ein Attributionsverfahren zumeist nicht mit linearen Beweisketten arbeiten kann. Vielmehr ergibt sich die Zuordnung aus dem Vergleich mit in der Vergangenheit gemachten Beobachtungen und dem Wiedererkennen von typischen Mustern und Vorgehensweisen (TTP, „*tactics, techniques and procedures*“). Selbst wenn sich in den forensischen Spuren also keine Namen, Adressen oder die sprichwörtliche ‚*smoking gun*‘ finden, wird die Qualität der Attribution umso besser und zuverlässiger, je häufiger ein Akteur beobachtet wird. Beim ersten Auftauchen wird es deshalb häufig nur bei einer „eher wahrscheinlichen“ Zuordnung bleiben, während ‚gute Bekannte‘ mit „hoher Wahrscheinlichkeit“ identifiziert werden können. Das Auswärtige Amt konsultiert gleichzeitig mit verbündeten Staaten. Dieser Austausch kann zuweilen durch im EU- und NATO-Kreis unterschiedlich gehandhabte Regeln für den Umgang mit vertraulichen Informationen erschwert werden. Die bisherige Erfahrung zeigt aber, dass Partnerinformationen für eine angemessene Bewertung unverzichtbar sind.

Anschließend wird der Kontext des Vorfalls im Ressortkreis diskutiert: seine politische Einordnung ebenso wie mögliche Auswirkungen von der unmittelbaren Gefährdung bis hin zum mittel- und langfristigen Schaden. Dafür spielt eine Rolle, welcher Art ein Angriff ist, was als Ziel und Erfolg des Angriffs gelten kann und wie er mit Blick auf international vereinbarte Normen zu bewerten ist. Der Vorschlag für die Reaktion auf den Vorfall wird durch das Auswärtige Amt erstellt. Der Vorschlag enthält eine Maßgabe zur Kommunikation in der Öffentlichkeit (ob und wie) und zur Information der Verbündeten (ob und wie). In der Vergangenheit löste ein nach außen intransparenter, langsamer Fortgang Irritationen insbesondere bei Verbündeten und Partnern aus, die sich Unterstützung durch Deutschland erhofften und auf diese teilweise lange warten mussten. Mit dem nun etablierten Verfahren sind sowohl Verfahrenssicherheit als auch ‚*Checks and Balances*‘ gewahrt, und es können Routinen etabliert werden, die zur erwünschten Beschleunigung führen.

Was ist Attribuierung nicht?

Das Attributionsverfahren der Bundesregierung sieht auf keiner Stufe einen Automatismus vor. So wird der Tatsache Rechnung getragen, dass es dem Erreichen politischer Ziele dient. Selbst, wenn die Urheberschaft für einen Vorfall eindeutig feststeht, kann es politische Umstände geben, unter denen es opportun erscheint, nicht zu attribuieren. Für politische Entscheidungsverantwortliche ist zudem wichtig zu verstehen, dass eine zu 100 Prozent sichere Identifizierung eines Angreifers im Cyberraum nur äußerst selten gelingt. Ohne eindeutige Beweise oder Bekenntnis des Täters muss das Bild aus verschiedenen Hinweisen zusammengetragen werden. So kann hinreichende und notwendige Plausibilität sichergestellt werden. Die verbleibende Unsicherheit sollte aber eine Attribution nicht ausschließen. Der nicht aufklärbare Rest an Unsicherheit und die damit möglichen Konsequenzen der Attribution sind in der politischen Verantwortung zu tragen. Ferner ist Attribution auch kein Teil des Krisenmanagements nach einem Cybervorfall, und es gibt somit auch keine Fristen, keinen Zwang oder Druck, das Verfahren möglichst sofort zu starten oder zeitnah abzuschließen.

Zugleich hat die Bundesregierung mit dem Attributionsverfahren klargestellt, dass es keine diplomatische Reaktion auf einen Cybervorfall ohne vorherige technisch-fachliche Attribuierung geben wird. Das Instrument ist also nicht in dem Sinne als „politisch" zu verstehen, dass es von sachfremden politischen Überlegungen gesteuert wäre. Es beruht, wie dies *Norm b* verlangt, auf der Faktenaufklärung zum Vorfall. Die Selbstbindung an diese Voraussetzung soll zur Deeskalation und Vertrauensbildung beitragen – auch als Signal an Dritte: Wenn ein Schuldiger benannt wird, dann liegt dem auch eine nachvollziehbare Indizienkette zugrunde. Wirbt Deutschland um solidarische Unterstützung, so können die Verbündeten davon ausgehen, dass es klare Hinweise auf den verantwortlichen Akteur gibt und sie diese auch einsehen können. Das Attributionsverfahren ist zudem von Verfahren der Strafverfolgung getrennt zu betrachten. Zwar können Erkenntnisse aus der Strafverfolgung hier einfließen, aber attribuiert werden kann auch ohne den Nachweis strafrechtlich relevanter Tatbestände. Auch umgekehrt muss nicht jede Strafverfolgung im Zusammenhang mit einem Cyberangriff aus dem Ausland zu einer Attribution führen. Diese hat ihren Einsatzbereich dort, wo es über die Ahndung eines Vergehens oder Verbrechens hinaus Anlass zu politischer Demarkation einer Normverletzung gibt.

Beispiel 1: Ghostwriter

Einige Monate vor der Bundestagswahl 2021 warnte das Bundesamt für Verfassungsschutz zusammen mit dem BSI Abgeordnete aus Bundestag und Landtagen, dass ihre E-Mail-Konten durch den Cyberakteur Ghostwriter kompromittiert seien, sensibilisierte für *Phishing-Mails* als gängigen Angriffsvektor dieser Gruppe und riet dazu, alle Passwörter auszutauschen, um den Eindringling auszusperren. Ghostwriter stand schon geraume Zeit vorher unter Beobachtung durch Cybersicherheitsbehörden und -unternehmen; die Spezialität der Gruppe ist die Verbindung von Cyberspionage mit Desinformationsoperationen. Beobachtet wurde die Vorgehensweise zuvor schon in Polen und im Baltikum, ebenfalls in Zusammenhang mit Wahlen. Dies war im Juni 2021 Thema sowohl im Außenministerrat der EU als auch im NATO-Rat.

Neben der direkten Ansprache der Opfer wurde auch ein Attributionsverfahren eingeleitet, das im Juli 2021 zum Abschluss kam. Nach einer direkten, nichtöffentlichen Ansprache Russlands, mit der versucht wurde, die Kampagne vor den Bundestagswahlen zu stoppen, attribuierte die Sprecherin des Auswärtigen Amtes in der Regierungspressekonferenz am 6. September öffentlich die Kampagne zu Russland. Am 24. September folgte die EU in Form einer Erklärung des Hohen Vertreters im Namen der EU, der sich unter anderen Norwegen und die Ukraine sowie weitere Partner anschlossen. Das Verfahren im Fall Ghostwriter verdeutlicht eine der Funktionen der Attribution: nämlich durch Identifizierung und Ansprache des verantwortlichen Staates einen möglichen Schaden abzuwenden – im besten Fall dadurch, dass die Einstellung der Kampagne erwirkt wird, hier durch eine Sensibilisierung von Medien und breiter Öffentlichkeit.

Beispiel 2: Viasat

In den frühen Morgenstunden des 24. Februar 2022 wurde die Software eines Modems für das KA-SAT-Kommunikationssatellitennetzwerks für Osteuropa mittels eines *Supply-Chain*-Angriffs gelöscht und Tausende Terminals fielen aus. Der Angriff erschwerte die militärische Kommunikation auf ukrainischer Seite während der russischen Invasion. Zugleich aber betraf der *Hack* auch zivile Einsatzbereiche des Satellitennetzes außerhalb der Ukraine, so zum Beispiel die Fernwartungssysteme des Windenergieanlagenherstellers ENERCON in Deutschland. Wegen dieses erheblichen Kollateralschadens startete die Bundesregierung ein Attributionsverfahren, obwohl der Angriff nicht in deutschen Netzen und nicht intentional gegen ein deutsches Ziel ausgeübt wurde. Die Risiken durch sogenannte *Spill-Over*-Effekte von Cyberangriffen, auch der Eskalation eines Konflikts durch Hineinziehen weiterer Parteien, werden in *Norm f* des VN-Expertenberichts sowie den angeschlossenen Erläuterungen thematisiert: *„A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."*

Die EU ging am 10. Mai 2022 mit einer Erklärung zur Verurteilung des Angriffs voran; die USA, Kanada, Großbritannien, Australien und weitere schlossen sich in eigenen Stellungnahmen an. Die Bundesregierung schloss das nationale Attributionsverfahren mit einer öffentlichen Übernahme der EU-Erklärung ab. Solidarität mit der Ukraine war sicher gemeinsame Motivation der Gruppe der attribuierenden Staaten, an dieser Stelle öffentlich zu werden. Es wurde aber auch herausgearbeitet, dass die Kollateralschäden des Cyberangriffs gegen die Ukraine von keinem der beteiligten Staaten als gegen sich selbst gerichtete kriegerische Handlung gewertet wurde. Eine Informelle Arbeitsgruppe der OSZE unter Vorsitz des ungarischen Botschafters Karoly Dan befasste sich mit dem Vorfall eine Woche später deswegen unter dem Vorzeichen von Vertrauensbildung: indem unter anderem Deutschland seine Analyse des Vorfalls offenlegte und seine Reaktion darauf erläuterte, stellte sich die Befassung mit dem Vorfall selbst als vertrauensbildende Maßnahme dar.

Beispiel 3: Albanien 2022

Am 15. Juli 2022 wurden die Netzwerke der albanischen Regierung Opfer eines Cyberangriffs, ausgehend von erfolgreichen *Ransomware*- und W*iper*-Angriffen auf einen zentralen IT-Serviceprovider. In von Albanien gemeinsam mit dem amerikanischen FBI durchgeführten Ermittlungen wurde Iran als Urheber identifiziert, was am 6. September zur Ausweisung aller iranischen Diplomaten aus Tirana und dem Abbruch der diplomatischen Beziehungen führte. Premierminister Edi Rama attribuierte den Vorfall am 7. September öffentlich zu Iran. Am 9. September, möglicherweise in Reaktion auf die Attribuierung, legte derselbe Akteur mit einem erneuten Angriff kurzzeitig die IT-Infrastruktur der albanischen Grenzkontrolle lahm.

Die Bundesregierung verurteilte den Angriff ohne eine öffentliche Attribuierung zu Iran am 7. September. Dies war der erste Fall einer nationalen Attribution ohne Betroffenheit deutscher IT-Infrastruktur. Eine Befassung des NATO-Rats diente der Klärung, dass die Bündnisfähigkeit Albaniens und die Sicherheit des Bündnisses an sich nicht betroffen waren, und mündete am 8. September in einer Erklärung der Solidarität mit Albanien, in der die NATO auch die albanische Attribution zu Iran anerkannte. Dieser Fall illustriert eine weitere Facette des Attribuierungskonzepts: *Norm b* kann auch gestärkt werden, ohne dass eigene Betroffenheit und eigene Erkenntnisse zum verantwortlichen Akteur vorliegen. Zur Geste der Solidarität, als welche die Verurteilung des Vorfalls zu verstehen ist, kommt hier noch praktische Hilfe durch Verbündete, sowohl bei der Untersuchung des Vorfalls, als auch bei der Wiederherstellung der IT-Infrastruktur, zum Zwecke der Wiedererlangung der Handlungsfähigkeit der albanischen Regierung.

Lessons learnt

Die bisher durchlaufenen Attributionsverfahren stellten für die Bundesregierung auch Lerngelegenheiten dar. Darauf aufbauend kann, muss und wird sich das Verfahren weiterentwickeln. Eine der wichtigsten Baustellen ist das Verfahren zum Teilen von Informationen, sowohl innerhalb der Bundesregierung als auch mit Partnern. Zentrale Informationen und Bewertungen unterliegen in Deutschland wie bei den Partnern der Geheimhaltung. Die Einstufung ist unumgänglich, verlangsamt und erschwert aber die Prozesse. Abhilfe könnte durch eine gemeinsame technische Plattform als Weiterentwicklung des gegenwärtig verwendeten Systems geschaffen werden. Für den Austausch mit Verbündeten existieren solche technischen Erleichterungen bisher nur im Ansatz, realisiert vor allem innerhalb der EU (INTCEN) und der NATO (BICES). Dazu kommen rechtliche Hürden sowie, insbesondere in Bezug auf nachrichtendienstliche Informationen, auch Vertrauensfragen, die Notwendigkeit des Quellenschutzes und Gegenseitigkeitserfordernisse.

Die Frage, wie Informationen geteilt werden, ist vor allem deswegen wichtig, weil ein Attributionsverfahren häufig auch unter Zeitdruck stattfindet: Die forensische Suche und Auswertung beanspruchen ihre Zeit, während der politische Druck, den Verursacher zu nennen, hoch ist. Wie im Fall von Ghostwriter kann zum Beispiel ein Privatunternehmen zwischenzeitlich mit Informationen an die Öffentlichkeit gehen, oder, wie im Fall von Albanien, drängt ein Partner auf rasche Fortschritte. Dennoch: Fehlnennungen und falsche Beschuldigungen sind zu vermeiden; sie schwächen die Glaubwürdigkeit des Attributionsverfahrens und *Norm b* an sich und geben all jenen Auftrieb, welche die Möglichkeit von Attribution bestreiten. Andererseits: Wenn Partner

oder Medien schneller sind und bereits an die Öffentlichkeit gehen, während das Verfahren noch läuft, erschwert das die weitere sorgfältige Analyse und reduziert die Aufmerksamkeit für diesen völkerrechtlich bedeutsamen Schritt. Die Herausforderung besteht darin, bei der Weiterentwicklung des Verfahrens beides im Blick zu behalten: so schnell wie möglich zu werden und dabei so gründlich wie nötig zu sein.

Noch nicht ausreichend konsolidiert ist allerdings die Terminologie der Attribution, und dies kann nicht innerhalb eines nationalen Attribuierungsverfahrens gelöst werden. Die Unschärfe beginnt bei der Begrifflichkeit selbst (Attribution oder Attribuierung, je nachdem ob Ergebnis oder Prozess betont werden) und setzt sich fort bei den verwendeten Qualifikatoren (politisch, technisch). Sie reicht aber auch in komplexe Fragen der Bewertung hinein, wenn es zum Beispiel um Wahrscheinlichkeiten geht: Eine Zuordnung kann (hinreichend) plausibel sein bis hin zu sicher. Insbesondere die Nachrichtendienste legen der Bewertung ihrer Informationen jeder seinen eigenen Maßstab zugrunde, und ebenso haben EU und NATO jeweils ihren eigenen Maßstab. Schließlich gibt es auch für die Klassifikation des Schadens durch einen Cybervorfall, der nach *Norm b* auch berücksichtigt werden soll, noch kein einheitliches Schema. Die Bundesregierung erläutert das in Deutschland genutzte Verfahren deshalb auch gegenüber internationalen Partnern und Verbündeten, zum Beispiel im Kreis der OSZE oder der NATO, um Transparenz herzustellen und Einfluss auf die Erwartungen zu nehmen, aber auch, um im Lauf der Zeit zu allgemein akzeptierten Mindeststandards für Attributionsentscheidungen zu kommen.

Die bisher mit dem Instrument der Attribution gemachten Erfahrungen legen nahe, keine allzu hohen Erwartungen in Bezug auf eine Verhaltensänderung beim böswilligen Akteur zu entwickeln. Insbesondere wird ein Angriff durch Attribution nicht gestoppt, da sie zumeist erst nach erfolgreicher technischer Intervention möglich ist. Attribution ist höchstens Teil der Abschreckung, aber auch hierfür nicht das am besten geeignete Instrument. Die Staaten, die bisher böswilliger Cyberangriffe bezichtigt wurden – Russland, China, Iran und Nordkorea – reagieren nicht oder im Gegenteil sogar eskalierend auf die öffentliche Nennung oder streiten die Verantwortung ab. Dies ist aber kein Grund, Attribution als Instrument aufzugeben. Zum einen zeigt die kleinteilige Diskussion um Formulierungen in der Auslegung von *Norm b* im VN-Expertenbericht von 2021 deutlich, dass auch diese Staaten eine gegen sie gerichtete Beschuldigung nicht einfach abschütteln. Ihr Ruf nach neutralen Verifikationsmechanismen zeigt, dass – nachdem die technische Forensik immer besser wird – die Legitimität des Attributionsprozesses an sich in Frage gestellt wird. Offenbar verursacht es politische Kosten, Gegenstand einer Attribution zu sein. Zum anderen lässt sich die Wirkung auf die ‚zweite Reihe' kaum messen: jene Regierungen, welche Cyberspionage und -sabotage in Erwägung ziehen, aber nicht die gleichen Ressourcen investieren können wie die genannten vier Staaten. Für sie muss die Aussicht, entdeckt und beschuldigt zu werden, Teil eines politischen Kalküls werden, bei dem es etwaigen Nutzen gegen Risiken für die bilateralen Beziehungen und das multilaterale *Standing* abzuwägen gilt.

In der Theorie setzt der reaktive Einsatz von „Cyberwaffen" (wie auch immer diese beschaffen sein mögen) die Identifikation des Cyberangreifers voraus, damit er als Selbstverteidigung oder Gegenmaßnahme im völkerrechtlichen Sinn gelten kann. Die öffentliche Nennung ist dafür nicht zwingend erforderlich. Nach innen muss es aber die Überzeugung geben, dass das Verfahren belastbare Zuweisungen hervorbringt und nicht unkalkulierbare Risiken birgt. Der Abschreckungseffekt der Attribution liegt daher nicht zuletzt in den Konsequenzen, die sie für die nationale Handhabung von Cyberfähigkeiten als Reaktion auf einen Angriff haben könnte. Für die Bundesregierung ist die Entscheidungsfindung in Bezug auf sogenannte aktive Abwehrfähigkeiten noch nicht abgeschlossen, und die Frage, wie sicher man sein kann, dabei ‚den Richtigen zu erwischen', spielt in dieser Diskussion eine große Rolle. Die Einübung des Attributionsverfahren und die Entwicklung von Vertrauen in dessen Ergebnisse sind deswegen Voraussetzung für Fortschritte in der Debatte.

Viele Staaten zögern, das Instrument im Alleingang zu nutzen, auch weil ihre eigenen Erkenntnisse möglicherweise nicht immer ausreichen, um plausible und glaubwürdige Zurechnungen vorzunehmen. Vielversprechend erscheint das wachsende Interesse innerhalb der NATO, Attribution gemeinsam vorzunehmen. Beim Warschau-Gipfel 2016 wurde erklärt, dass auch Cyberangriffe einem bewaffneten Angriff gleichkom-

men und den Bündnisfall auslösen können. Dies würde erfordern, dass der betroffene Staat oder die betroffenen Staaten ihre Erklärung gegenüber den Verbündeten substantiieren. Zwar mag der NATO die detaillierte *Toolbox* der EU fehlen, aber sowohl über eigene Reaktionsmöglichkeiten im Bündnis als auch über die Weiterentwicklung der NATO-EU-Zusammenarbeit in diesem Bereich sollte man nachdenken.

Kopfzerbrechen verursacht weiterhin die Beobachtung, dass auch eine gründlich vorbereitete Attribution nicht verhindern kann, dass der beschuldigte Staat die Verantwortung abstreitet und die Attribution als solche damit droht, zur Pflichtübung zu werden, ohne weitere Folgen zu zeitigen. Es gibt derzeit vor allem zwei Überlegungen, dieser Entwicklung entgegenzutreten. Zum einen könnte Attribution in breitere politische Dialoge eingebettet werden, insbesondere dann, wenn Staaten auf ‚*naming and shaming*' unempfindlich oder auch überempfindlich reagieren. In einem solchen Dialog könnte nämlich der mittel- und langfristige Schaden von Cyberspionage oder -sabotage auf das bilaterale Verhältnis oder auch die internationale Anerkennung thematisiert werden. Ein solcher, möglicherweise auch mit ‚Zuckerbrot' unterlegter Appell zur Verhaltensänderung wäre eine strategischere Herangehensweise als die jeweils für sich stehende Attribution beziehungsweise, wie in einigen Fällen absehbar, die wiederholte Attribution zum selben Akteur, die folgenlos bleibt.

Zum anderen könnten Staaten auch an ihrer ‚Peitsche' arbeiten und eine Attribution mit stärkeren Sanktionen verknüpfen, als sie in der EU-*Cyber Diplomacy Toolbox* enthalten sind. Mit EU-Cybersanktionen können bisher Individuen oder Entitäten belegt werden, doch sind die Hürden des Nachweises der Verantwortung recht hoch und die Strafwirkung dabei recht gering, da auf die Ebene von einzelnen Personen beschränkt. Denkbar wären hier beispielsweise Sektorsanktionen sowie gemeinsame Sanktionen mit Drittstaaten außerhalb der EU, um Möglichkeiten zum Umgehen der Sanktionen zu verringern.

Wenngleich Attribution bisher vor allem im geopolitischen Kräftefeld zwischen den USA, der EU, China und Russland stattgefunden hat, sollte auch die Perspektive des globalen Südens berücksichtigt werden. Mit dem Fokus auf die Bekräftigung globaler Normen gewinnt das Instrument für die ‚*non-aligned*'-Staaten an Bedeutung. Für sie wird deutlich, dass die Normen für verantwortliches Staatenverhalten im Cyberspace auch dazu dienen, dass digitale Transformation weiter ein Erfolgsrezept für Entwicklung bleibt. Attribution unterstützt den Prozess der Verregelung des Cyberspace auf dem Weg vom Wilden Westen zu einem Ökosystem, in dem viele verschiedene *Player* ihren Platz und ihr Auskommen finden und kollektive ebenso wie individuelle digitale Rechte geschützt sind.

Dr. Regine Grienberger ist Cyberbbotschafterin im Auswärtigen Amt. Die Autorin gibt ihre persönliche Meinung wieder. *Alle Fallbeispiele können in der Datenbank http://eurepoc.eu eingesehen werden.*

Alle Ausgaben der Arbeitspapiere Sicherheitspolitik sind verfügbar auf:
www.baks.bund.de/de/service/arbeitspapiere-sicherheitspolitik